Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt : Petter Andreas Bergh
Telefon: 92032532

Eksamen i MA1301 Tallteori

Bokmål
Torsdag 9. desember 2010
Kl. 15.00–19.00 (4 timer)

Hjelpemidler: kode D (bestemt enkel kalkulator: HP30S eller Citizen SR-270X)

Alle svar skal begrunnes.

Oppgave 1 Finn alle løsninger av systemet

$$\begin{aligned} x &\equiv 3 \pmod 8 \\ x &\equiv 9 \pmod{11} \\ x &\equiv 4 \pmod 7 \end{aligned}$$

Hva er den minste positive løsningen?

Oppgave 2 Hva får vi til rest når vi deler $65! + 70$ på 67?

Oppgave 3 Vis at det finnes uendelig mange primtall p med $p \equiv 3 \pmod 4$.
Hint: $4p_1p_2 \cdots p_t - 1$.

Oppgave 4 Alice konstruerer et RSA-kryptosystem med primtallene 7 og 23, og da med $n = 7 \cdot 23 = 161$. Som offentlig nøkkel velger hun $\{n, e\} = \{161, 25\}$.

a) Hva blir den hemmelige nøkkelen $\{n, d\}$?

b) Bob vil sende meldingen $M = 2$ til Alice. Krypter denne meldingen.

Oppgave 5 La p og q være to ulike primtall. Vis at $\sqrt{pq}$ er et irrasjonalt tall.

Oppgave 6 Etter en Wannskrækk-konsert på Samfundet i 1980 ble det oppdaget at alle inngangspengene var stjålet. Da politiet kom husket ikke kassereren nøyaktig hvor mye penger det var snakk om, bare at det var mer enn 38100 kroner og mindre enn 38130 kroner. Konserten kostet 34 kroner for Samfundet-medlemmer og 85 kroner for ikke-medlemmer. En tallteoristudent som sto like ved kunne straks fortelle at det nøyaktige beløpet må ha vært 38114 kroner.

a) Begrunn hvorfor det ble betalt inn nøyaktig 38114 kroner i inngangspenger.

b) Antall Samfundet-medlemmer på konserten var minst 900 og ikke mer enn 905. Nøyaktig hvor mange Samfundet-medlemmer og hvor mange ikke-medlemmer var det på konserten? Vi regner bare med de som betalte.

Oppgave 7 Vis at 2010 deler $13^{528n} - 1$ for alle $n \geq 1$.

Oppgave 8 La p og q være to tvillingprimtall. Vis at den kvadratiske kongruensen

$$x^2 \equiv p \pmod{q}$$

er løsbar hvis og bare hvis den kvadratiske kongruensen

$$x^2 \equiv q \pmod{p}$$

er løsbar.